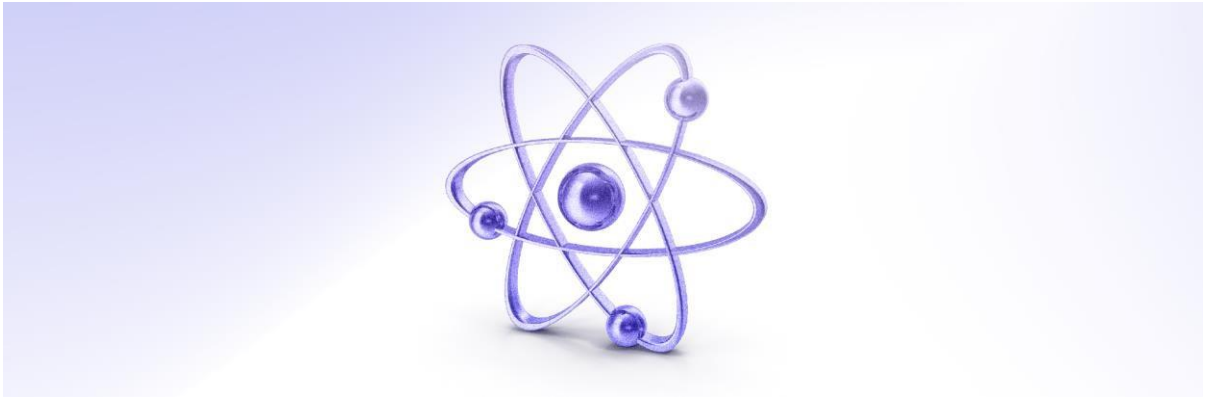
FS-ISAC | Security Tips Newsletter

JTNB Jim Thorpe Neighborhood Bank

19 August 2024 | Issue No. 12

Security is Everyone's Responsibility

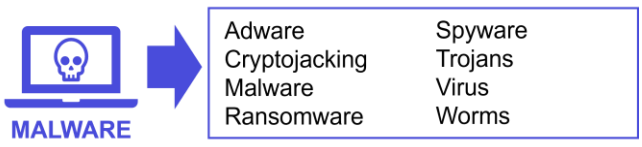


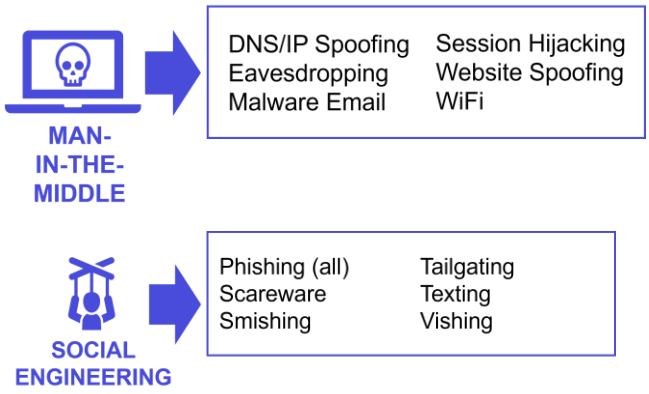
Understanding Cyber Threats

The one thing cybersecurity threats have in common is that they are harmful and the cybercriminal is committed to destroying, stealing, or disrupting data, critical systems, and digital life in general. Your financial institution uses numerous security applications and incorporates processes to keep your financial information and assets secure and to comply with regulatory guidelines.

However, security is everyone's responsibility, and you can do the following three things to help safeguard your assets.

First, educate yourself about the various tactics, techniques, and processes (TTP) cybercriminals use to steal from you. TTPs are like fashion – what's in style one month is out-of-date the next – so cybercrimes change over time. Below you'll see the most current attack types and TTPs.





Second, install security applications on your personal computers and mobile devices. Those applications – especially anti-virus and content-blocking applications – are an additional layer of protection for devices connected to the outside world. It's important to secure all your devices, especially those used by your whole family.

As tempting as free security applications are, they aren't always the best way to protect your financial data. Research and select applications offering the best protection. Consider it an investment that protects you from the hassles of restoring your online financial life to some degree of normal.

Third, regularly monitor your account activity and tell your financial institution about suspicious activity. Many financial services providers offer mobile apps that alert you to activity on your accounts. Those apps help you and your institution remediate cybercrime quickly.

Tips To Help You Remain On Guard

- Don't reveal personal or financial information in a text or email, and don't respond to email solicitations for this information.
- Don't click on links sent in a text or email – you might wind up in a scam site built by a cybercriminal.
- Don't send sensitive information over the internet without checking the website's security. Look for URLs that begin with "https" – the 's' stands for secure – rather than "http." A website safety checker like Google Safe Browsing helps, too.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your institution, contact them immediately. IC3.gov and the

TLP WHITE

12120 Sunset Hills Rd, Reston VA 20190